BY ORDER OF THE COMMANDER

DOVER AIR FORCE BASE INSTRUCTION 33-104

8 DECEMBER 2000

Communications and Information

NETWORK OPERATIONS AND SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://afpubs.hq.af.mil.**

OPR: 436 CS/SCB (SMSgt West) Certified by: 436 CS/CC (Lt Col Linda R. Medler)
Supersedes DAFBI 33-104, 12 October 1999 Pages: 21
Distribution: F

This instruction implements Dover AFB policy on network operations and security as directed by the 436th Communications Squadron. It outlines responsibilities and directives to operate computers and associated devices on the Dover AFB network. It applies to all organizations and individuals that use government computer systems on Dover Air Force Base.

SUMMARY OF REVISIONS

This revision updates the electronic mail area, providing specific guidance for naming conventions and paragraph **8.**, restricting the size of personal drives and file extensions on shared drives. It adds procedures and responsibilities for software management. It further adds responsibilities for the Network Control Center.

1. Introduction.

1.1. This base instruction provides definitive guidance on how to securely employ and efficiently manage information systems on the network. It outlines roles and responsibilities for each level of information system user and manager IAW existing AFIs. These procedures and guidelines supplement existing Air Force guidance and provide detailed operating procedures for all Dover AFB information system users to follow.

2. Background.

2.1. While the Air Force has developed a myriad of instructions and guidelines defining the rules associated with networks, their broad nature has left significant room for interpretation at base level. Due to the increased dependence and mission criticality of our information systems, their security and efficient management is vital to mission accomplishment. This instruction provides the means and rationale for actions required to ensure computer security and effective network management.

3. Security.

3.1. User Responsibilities.

3.1.1. Users of stand-alone or network computer systems will comply with the following:

3.1.1.1. Screensavers/Lock workstations.

3.1.1.1.1. Enable password protected screensavers or lock workstations immediately when left unattended.

3.1.1.1.2. If multiple users access the same computer system and individual screensavers are not available, each user must logout when leaving the computer system.

3.1.1.2. Anti-virus Software.

3.1.1.2.1. The base standard anti-virus software will be installed on every computer system and configured to scan all files, folders and messages daily as a minimum.

3.1.1.2.2. Anti-virus software updates will be installed upon distribution on the DAFB Intranet.

3.1.1.2.3. Anti-virus software installed and configured by the user, Unit FA/WGA or 436 CS personnel will be set to scan all removable media (i.e. - floppy disks, CDs, etc.) prior to use.

3.1.1.2.4. The base standard anti-virus software is licensed for home use to preclude virus propagation outside the office and should be installed and updated accordingly. The 436 CS will publish the latest version in use on the Dover AFB web page at **http://wwwmil.dover.af.mil**.

3.1.1.3. Authentication and Identification.

3.1.1.3.1. IAW AFMAN 33-223, *Identification and Authentication*, all computer system passwords will be no less than 8 characters in length and consist of numbers, letters (upper & lower case) and at least one special character. Passwords not meeting criteria identified by AFMAN 33-223 will be rejected and will result in the 436 CS denying users network access.

3.1.1.3.2. Users will protect and not disclose their passwords to anyone. Users will be held accountable for all workstation or network activities that take place on their account.

3.1.1.3.3. Generic accounts (generically named account used by various personnel) are prohibited on the network.

3.1.1.3.4. All users requiring a network account must process through the Network Accounts office. Users will be required to complete initial training and sign a user agreement (**Attachment 1**) before an account will be established.

3.1.1.3.5. All outbound personnel with network accounts must out-process through the Network Accounts office.

3.1.1.4. Security Awareness, Training and Education (SATE).

3.1.1.4.1. IAW AFI 33-204, *Information Protection, Security Awareness, Training and Education (SATE) Program*, all users that access stand-alone or network computer systems must complete SATE on an annual basis. The SATE program can be accessed on the Dover AFB web page at **http://wwwmil.dover.af.mil**.

3.1.1.4.2. Users must complete SATE annually to maintain network access.

3.1.1.5. Games.

3.1.1.5.1. No games are authorized on any government computer system.

3.1.1.6. Modems.

3.1.1.6.1. Modems on computer systems attached to the network are prohibited. Users requiring modems must gain approval by submitting initial or updated Certification & Accreditation (C&A) documentation to 436 CS/SCBI, Information Assurance Office for approval/disapproval by the Designated Approval Authority (DAA). Users requiring remote access through a dial-in account must submit their requirement via AF Form 3215, **C4 Systems Requirements Document**, to 436 CS for approval/disapproval.

3.1.1.7. Peer-to-Peer Networks.

3.1.1.7.1. Peer-to-peer networks are prohibited. However in some cases peer to peer relationships may be used for some services that are not provided centrally (e.g. print services). Users requiring peer-to-peer networks must gain approval by submitting initial or updated C&A documentation to 436 CS/SCBI for approval/disapproval by the DAA.

3.1.1.8. Data Backup.

3.1.1.8.1. Backup of individual data is incumbent on the individual user.

3.1.1.9. Internet and Web Services.

3.1.1.9.1. Internet daemons (a program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur) on computer systems are prohibited. Users requiring Internet daemons must gain approval by submitting initial or updated C&A documentation to 436 CS/SCBI for approval/disapproval by the DAA.

3.1.1.9.2. Users will not knowingly access web sites that automatically store or install data/programs on their computers.

3.1.1.9.3. Use of Internet information sources such as commercial e-mail services, chat rooms, web-based bulletin boards and newsgroups are prohibited. Users requiring access to these information sources must submit their requirement via AF Form 3215, **C4 Systems Requirements Document,** to 436 CS for approval/disapproval.

3.1.1.9.4. The Network Control Center (NCC) will operate the base's only web servers.

3.2. Workgroup Administrator (WGA) And Functional Systems Administrator (FSA) Responsibilities.

3.2.1. WGAs and FSAs are responsible for educating and ensuring all their users comply with applicable instructions and guidelines, to include those in paragraph **3.1.** WGAs and FSAs are responsible for ensuring compliance with the following:

3.2.1.1. Certification & Accreditation (C&A).

3.2.1.1.1. C&A documentation will be completed for stand-alone computers, network workstations/servers and all other information systems (i.e. centrally managed systems) utilizing Dover network infrastructure. C&A documentation will be submitted to the Wing Information Assurance Office for approval/disapproval by the DAA prior to system installation and use.

3.2.1.1.2. Connection of any computer system to the network is contingent upon proper system configuration and C&A. For Newly purchased workstations may be connected if they comply with existing network configuration standards. The unit CSSO will ensure workstations meet NCC standards and make updates to the C&A package. Mission systems will not be connected until having gone through the C&A process and approved by the DAA.

3.2.1.1.3. Any hardware or software changes to a computer system require updates to C&A documentation.

3.2.1.1.4. Full C&A packages must be reviewed annually and expire every 3 years. Interim C&As expire annually.

3.2.1.2. Ports & Protocols.

3.2.1.2.1. Internet Protocol (IP) is the supported and prevalent protocol on the network.

3.2.1.2.2. All required ports and protocols will be documented in C&A documentation.

3.2.1.2.3. Ports and protocols prohibited by AFSSI 5027 will not be enabled on the network without prior Air Force Communications Agency (AFCA) waiver and DAA approval.

3.2.1.2.4. Port and protocol availability and supportability is subject to change per Air Force Computer Emergency Response Team (AFCERT) notification.

3.2.1.3. Network Security Scans.

3.2.1.3.1. Computer systems with high-risk vulnerabilities identified in network security scans must be corrected within 5 duty days or they will be disconnected from the network.

3.2.1.3.2. Computer systems with medium risk vulnerabilities identified in network security scans must be corrected before the next network security scan or they will be discon-

nected from the network.

3.2.1.4. Air Force Computer Emergency Response Team (AFCERT) Advisories.

3.2.1.4.1. WGAs/FSAs will correct computer (local workstations and centrally managed systems) vulnerabilities IAW the AFCERT Advisory as soon as possible. Status reports must be sent to the Wing Information Assurance (IA) Office every Wednesday until compliance is accomplished. Status reports must include ECD and rationale for extended non-compliance, as well as justification for negative or N/A responses.

3.2.1.4.2. WGAs and FSAs will establish controls to track compliance status on all workstations within their organization, to include new workstations as they are installed**.** As a minimum, compliance status data collection will contain the fields referenced in **Attachment 2**.

3.2.1.5. AFCERT Compliance Message (ACM).

3.2.1.5.1. WGAs/FSAs will correct computer (local workstations and centrally managed systems) vulnerabilities IAW the ACM within 12 calendar days from the date of the ACM. Status reports must be sent to the Wing IA Office every Wednesday until compliance is accomplished. Status reports must include ECD and rationale for suspense extensions, as well as justification for negative or N/A responses.

3.2.1.5.2. WGAs and FSAs will establish controls to track compliance status on all workstations within their organization, to include new workstations as they are installed**.** As a minimum, compliance status data collection will contain the fields referenced in **Attachment 2**.

3.2.1.5.3. WGAs and FSAs will ensure all applicable software, patches and fixes are installed on a workstation within 5 duty days of the workstation being placed in active service. NCC personnel will notify WGAs/FSAs when a workstation is found to be deficient. Workstations found to have repeat deficiencies will have network access administratively disabled until required software, patches and fixes are applied.

3.3. Network Control Center (NCC) Responsibilities.

3.3.1. The NCC is responsible for disseminating network management and security information to WGAs, FSAs and the DAA. The NCC will enforce all instructions and guidelines, to include those in paragraph **3.1.** and paragraph **3.2.** Additionally, the NCC is responsible for the following:

3.3.1.1. Anti-virus Software.

3.3.1.1.1. The base standard anti-virus software and associated update files will be made available on the Dover AFB web page or shared drives for base implementation.

3.3.1.2. Authentication & Identification.

3.3.1.2.1. The NCC will ensure password-checking software is in place to prevent users from creating non-compliant passwords. The NCC will scan all network passwords for compliance quarterly.

3.3.1.3. Security Awareness and Training Education (SATE).

3.3.1.3.1. Network accounts will be established with a 365-day expiration date, contingent upon users completing their annual SATE requirements.

3.3.1.4. Certification and Accreditation (C&A).

3.3.1.4.1. No computer system will be enabled on the network without C&A documentation approved by the DAA. The Wing Information Assurance office located in the 436 CS can provide assistance to accomplish this.

3.3.1.4.2. C&A documentation will be reviewed annually for changes and expiration.

3.3.1.5. Ports and Protocols.

3.3.1.5.1. Prohibit all unapproved port activity and ensure compliance with AFSSI 5027.

3.3.1.6. Network Security Scans.

3.3.1.6.1. Conduct network security scans monthly. Ensure high and medium risk vulnerabilities are corrected or the risks minimized IAW paragraph **3.2.1.3.** These scans will also be used to verify closure of AFCERT Advisories and ACMs.

3.3.1.6.2. Post network security scan results on the web for WGA, FSA and DAA review and action.

3.3.1.6.3. Monitor fix actions for high and medium risk vulnerabilities and take appropriate actions IAW paragraph **3.2.1.3.** as required.

3.3.1.7. Games.

3.3.1.7.1. Remotely remove any games discovered on government computer systems.

3.3.1.8. Modems.

3.3.1.8.1. Conduct quarterly scans to detect illegal modems.

3.3.1.8.2. Disable network access for any computer systems with illegal modems.

3.3.1.8.3. Provide a central and single Remote Access Server capability to the base.

3.3.1.9. Data Backup.

3.3.1.9.1. Complete full server backups of configuration and data weekly, with incremental backups daily. Backups will be stored at an alternate location separate from the NCC. Backups will be rotated on a monthly basis.

3.3.1.9.2. Ensure the integrity of the entire server before exercising restoral efforts for an individual(s).

3.3.1.10. Internet and Web Services.

3.3.1.10.1. At the web proxy server, block offending web sites to include those specifically targeted in AFI 33-129, *Transmission of Information Via the Internet,* and those in paragraph **3.1.1.9.**

3.3.1.11. Internet Protocol (IP) Bulletins.

3.3.1.11.1. NCC will block all IP Bulletin IP addresses at the base and Medical Group routers as they are released.

4. Electronic Mail.

4.1. User Responsibilities.

4.1.1. IAW 33-119, *Electronic Mail (E-mail) Management and Use,* e-mail will be used only for official and authorized purposes. Inappropriate use will result in disabled e-mail accounts until the offender's commander sends a written request for reactivation to 436 CS/CC or 436 CS/SCB.

4.1.2. Mass broadcast e-mails are not authorized. E-mails may only be sent to squadron or smaller distribution lists. The only exceptions are to notify personnel of imminent danger to base resources. Offenders will have their e-mail accounts disabled until their commander sends a written request for reactivation to 436 CS/CC or 436 CS/SCB.

4.1.3. Users will mass distribute information by forwarding their e-mail to appropriate POCs in each organization for distribution within their respective unit.

4.1.4. IAW 33-119, chain letters are prohibited. Offenders will have their e-mail accounts disabled until their commander sends a written request for reactivation to 436 CS/CC or 436 CS/SCB.

4.1.5. E-mail attachments will be no larger than 2Mb. The NCC, at extension 2666, will address alternative solutions on a case-by-case basis.

4.2. Network Control Center (NCC) Responsibilities.

4.2.1. NCC will restrict e-mail attachment sizes to 2Mb.

4.2.2. NCC will disable e-mail accounts of those individuals that violate pertinent AFIs and guidelines addressed in this instruction.

4.2.3. To preserve and maintain adequate storage space on the e-mail servers, user e-mail INBOX size will be limited to the following:

Users - 20Mb

Squadron Commander - 100Mb

Deputy Group/Group/Wing Commander - Unlimited

4.2.3.1. Requests to increase e-mail INBOX must be documented on an AF Form 3215, C4 Systems Requirements Document and coordinated through the respective WGA for 436 CS/SCB approval/disapproval.

4.2.4. NCC will ensure the standard format for an individual e-mail address is "firstname.lastname@base.af.mil." Hyphenated names remain hyphenated with a period between the first and last name. Apostrophes are not permitted. Nicknames and nonofficial names are not permitted.

4.2.5. NCC will ensure the standard format for organizational e-mail addresses is "org.office@base.af.mil." For example, the Commander, 436th Airlift Wing is represented as "**mailto:436AW.CC@dover.af.mil**."

4.2.6. NCC will ensure the standard Air Force display naming convention is "last name, first name, middle initial, generation qualifier, rank, organization, and office. The elements are separated by a space, and punctuation, including commas, is not permitted. The syntax is <Lastname Firstname Middleinitial Generationqualifier Rank Organization/Office>. For example: Davis Sam E Jr GS-12 AF/SCXX.

5. Internet and The Worldwide Web.

5.1. User Responsibilities.

5.1.1. IAW 33-129, *Transmission of Information Via the Internet*, accessing inappropriate sites and distributing offensive material via e-mail (pornographic, racism or hate literature, etc.) is not authorized. As violators are identified, evidence will be forwarded to their commander for disciplinary action.

5.2. Pagemaster Responsibilities.

5.2.1. Unit pagemasters will be the only publishers to their unit's website.

5.2.2. Unit pagemasters will coordinate any publicly accessible web pages with public affairs before publishing.

5.2.3. No operationally sensitive information will be published on publicly accessible web pages.

5.2.4. All web pages will conform to the standards set forth in Dover Supplement AFI 33-129 and Dover AFB Handbook 33-129.

5.2.5. All references to commercial entities and organizations must be relevant to the content of the page and prefaced with a non-endorsement statement.

5.2.6. Unit pagemasters will protect their web server accounts and not distribute their user ID or passwords to anyone.

5.2.7. Unit pagemasters will coordinate all scripting with NCC personnel.

5.3. Network Control Center (NCC) Responsibilities.

5.3.1. The NCC will maintain the only base web servers. The NCC will maintain the operation of the web servers and have oversight into everything published on the web server.

5.3.2. Will give web server access to only those pagemasters appointed in writing.

5.3.3. Will allot 20Mb of space for each unit's web page. Additional space may be requested by submitting an AF Form 3215 from the unit's pagemaster to 436 CS/SCB.

5.3.4. Ensure that only DoD organizations on Dover AFB will have web sites on the base web server.

5.3.5. Periodically monitor web server logs for access to inappropriate sites. NCC will forward evidence to offending unit's commander for disciplinary action. If no action is noted in 7 days, the offending workstation's network access will be disabled until the offending unit's commander indicates that appropriate action has been taken.

5.3.6. NCC will block inappropriate site access as those sites are discovered.

5.4. Commanders Responsibilities.

5.4.1. Appoint in writing a pagemaster and an alternate responsible for creating and maintaining their unit's web page. Send the appointment letter to the Base webmaster located at the 436 CS/SCBS.

6. Training.

6.1. User Responsibilities.

6.1.1. All network users will attend the Communications Squadron Network Familiarization Class before obtaining a network account. Upon completion, users must sign a licensing agreement (**Attachment 1**) that outlines their training and their network responsibilities.

6.2. Functional Systems Administrator (FSA) Responsibilities.

6.2.1. The functional unit or community is responsible for FSA training on a centrally managed or functional system.

6.2.2. Network and computer system training will be completed following WGA guidelines in paragraph **7.3.** and IAW 33-115V2*, Certifying Network Professionals and Licensing Network Users* (DRAFT).

6.3. Workgroup Administrator (WGA) Responsibilities.

6.3.1. IAW the 436 AW WGA Training Plan, WGAs will complete all Computer Based Training (CBT) requirements IAW AFI 33-115V2 (Draft). In lieu of the MS Office application CBTs, WGAs may attend locally taught courses through the 436 CS. Additionally, WGAs must attend local WGA classes taught by the 436 CS. The 436 CS will provide WGA'srefresher training on an as needed and space available basis. Commercial classes may be taken at the owning unit's expense. The 436 CS is responsible for maintaining the WGA training program.

6.4. Commander Responsibilities.

6.4.1. Unit commanders must ensure their WGAs are directed and given the opportunity to attend and complete WGA training requirements.

6.4.2. Unit commanders will manage their WGAs to ensure continuous coverage.

6.5. Network Control Center (NCC) Responsibilities.

6.5.1. The NCC will conduct WGA training classes for military and civilian personnel consistent with those requirements outlined in the 436 AW WGA Training Plan.

6.6. Functional Manager Responsibilities.

6.6.1. The 3A0X1 Functional Manager will monitor the progress and WGA training status of those 3A0X1s assigned WGA duties.

7. Technical Support.

7.1. User Responsibilities.

7.1.1. Contact their unit FSA or WGA (as appropriate) first for computer systems support. If the WGA is unavailable and the outage presents a work stoppage requiring immediate technical support, contact Comm Customer Service at x2666.

7.2. Workgroup Administrators (WGA) AND Functional Systems Administrators (FSA) Responsibilities.

7.2.1. Ensure all customers are aware of the WGA and FSA computer support role.

7.2.2. Maintain and configure all unit computer systems and associated software IAW 33-115V1, *Network Management*.

7.2.3. Follow and enforce guidance from the NCC on network and computer security, configuration, acquisition and standards.

7.2.4. Serve as the unit Focal Point to Comm Customer Service in resolving computer system problems.

7.2.5. Provide on-site assistance when NCC personnel are dispatched to resolve computer system problems.

7.3. Communications Customer Service (CCS) Responsibilities.

7.3.1. Provide over-the-phone assistance to WGAs , FSAs and users when applicable (per paragraph **7.1.1.**) in resolving computer system problems.

7.3.2. Maintain current listings of unit WGAs and FSAs.

7.3.3. Dispatch appropriate NCC technician(s) when over-the-phone support proves inadequate.

7.4. Network Control Center (NCC) Responsibilities.

7.4.1. Provide last level of on-base support to resolve computer system problems or issues.

7.4.2. Addresses computer system problems or issues as assigned by CCS.

7.4.3. Perform preventive maintenance on every non-512 AW (AFRC) Unit Training Assembly Sunday from the hours of 0600-1100. Unit WGAs/FSAs will be notified 72 hours prior to any preventive maintenance weekend.

7.4.4. Shut down all network servers and associated equipment if the ambient room temperature in the NCC exceeds 85 degrees Fahrenheit. The 436 CS will notify 436 CES, 436 AW/CP and send out a network broadcast message to notify users of the imminent outage.

7.5. Commander Responsibilities.

7.5.1. Appoint in writing at least one WGA and an FSA (as appropriate) with at least one alternate (see **Attachment 4** and **Attachment 4**).

7.5.2. Ensure that either the primary or alternate WGA and/or FSA is available to address unit computer system problems or issues.

7.5.3. Ensure unit members utilize their WGA and/or FSA to the fullest extent possible and only call Comm Customer Service on computer system problems when situations arise as stated in **7.1.1.**

7.5.4. Appoint in writing a replacement WGA or FSA 60 days prior to the incumbent's PCS, separation, retirement or reassignment.

8. Standards.

8.1. Standards for the base network and associated workstations are in place to facilitate the greatest degree of interoperability and maintainability. Adherence to these standards is mandatory, although exceptions may be requested on a case-by-case basis by submitting an AF Form 3215, **C4 Systems Requirements Document**, to the 436 CS.

8.2. Internet Protocol (IP) Address Management.

8.2.1. The NCC will allocate blocks of IP addresses to organizational WGAs. They will assign them to devices using the following guidelines:

Device	IP Addresses
Network (Router and File Servers)	XXX.1 to XXX.15
Printers	XXX.16 to XXX.35
Hosts (Workstations)	XXX.36 to XXX.235
Network Maintenance	XXX.236
Network Switches	XXX.237 to XXX.249
Network Hubs	XXX.250 to XXX.254

Exceptions to these guidelines should be coordinated with the NCC.

8.3. Host Name Assignment.

8.3.1. NCC, WGAs and FSAs will assign host names using the following guidelines:

Device	Host Name
Network (Router and File Servers)	Coordinate with NCC
Printers	(Bldg #)”ptr”(IP #)
Hosts (Workstations)	(Bldg #)(Org)(IP #)
Network Maintenance	(Subnet)”mx236”
Network Switches	(Bldg #)(Subnet)”m” or “s1” thru “s12”
Network Hubs	(Bldg #)(Subnet)”m” or “s1” thru “s4”

Exceptions should be coordinated with the NCC.

8.4. NETWORK PERSONAL AND SHARED DRIVE RESTRICTIONS

8.4.1. Network personal drives will be limited to the following standard:

Wing Staff (CC, CV, DS, CCE, CCS, FA): Unlimited
Group CCs and CDs: Unlimited
Squadron CCs: 250M
1st Sergeants: 100M
Other Users: 5M

Exceptions should be coordinated with the NCC.

8.4.2. Music, video, or picture files (.wav, .avi, or .jpg, and .mpg respectively) may not be saved on personal drives unless they are for official use and then only for a limited time. The NCC reserves the right to delete files that are obviously not of an official nature, or when server space shortages warrant their removal.

8.4.3. Email files (.pst) may not be saved on shared drives. Exceptions will be made on a case-by-case basis if mission warrants.

8.5. User And WGA/FSA Responsibilities.

8.5.1. All computer systems will comply with the NCC Network and Workstation Standards located with the base Equipment Control Officer and on the Dover AFB web page.

8.6. NCC Responsiblities.

8.6.1. NCC with the approval of the DAA has the authority to allow downward directed and other information systems connectivity to the base network.

8.6.2. NCC will keep NCC Network and Workstation Standards current and up-to-date.

8.6.3. NCC will block all .pst files from being saved onto shared drives

9. Services.

9.1. IAW 33-115V1 and local policies, the NCC will maintain and be the sole source for providing the following common services to the base:

- Domain Name Services (DNS)
- Windows Internet Name Services (WINS)
- Messaging (Defense Message System (DMS), E-mail, Automated Digital Network (AUTODIN)
- Shared File/Print Services
- Off-base Connectivity (Non-secure Internet Protocol Routed Network (NIPRNET)/Secure Internet Protocol Routed Network
(SIPRNET)/Internet)

- Web Server
- Internet Protocol (IP) Address Management
- Remote Dial-in
- Distributed Printing
- Network Time Protocol
- Network Directory Services (NDS)
- Network Infrastructure (switches, routers, hubs, inter-building connectivity)

S. TACO GILBERT III, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFMAN 33-223, *Identification and Authentication*, 1 Jun 98

AFI 33-204, *Information Protection Security Awareness, Training and Education (SATE) Program*, 26 Apr 99

AFSSI 5027, *Network Security Policy*, 27 Feb 98

AFI 33-129, *Transmission of Information Via the Internet*, 1 Jan 97

AFI 33-119, *Electronic Mail (E-mail) Management and Use*, 1 Mar 99

AFI 33-115V1, *Network Management*, 1 Jun 98

AFI 33-115V2 (DRAFT), *Certifying Network Professionals and Licensing Network Users*, 1 Feb 99

Abbreviations and Acronyms

IAW—In Accordance With

AFI—Air Force Instruction

SATE—Security Awareness, Training and Education

C&A—Certification and Accreditation

DAA—Designated Approval Authority

CSRD—C4 Systems Requirements Document

NCC—Network Control Center

WGA—Workgroup Administrator

FSA—Functional System Administrator

AFCA—Air Force Communications Agency

AFCERT—Air Force Computer Emergency Response Team

ECO—Equipment Control Officer

DNS—Domain Name Services

AUTODIN—Automated Digital Network

DMS—Defense Message System

SIPRNET—Secret Internet Protocol Router Network

NIPRNET—Non-Classified Internet Protocol Router Network

NDS—Network Directory Services

IA—Information Assurance

NTP—Network Time Protocol

IP—Internet Protocol

AFSSI—Air Force Systems Security Instruction

Terms

Accreditation—Formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls.

Certification—Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Daemon—A background process that performs a system-related task.

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

Functional System Administrator (FSA)—FSAs are not assigned to the NCC however, as part of the network team, they still take direction from the NCC, which has the lead. They must thoroughly understand the customer's mission and stay completely knowledgeable of the hardware and software capabilities and limitations. The FSA's area of responsibility is from the user's terminal to the server, but does not include the network backbone infrastructure components. FSAs ensure servers, workstations, peripherals, communications devices and software are on line and available to support customers. Transfer of FSA responsibilities for functional area LANs to the NCC can occur if a memorandum of understanding, memorandum of agreement or service level agreement outlining the terms and conditions is signed between the NCC provider and the recipient. NCC NAs do not operate the end-users' application software, perform data entry, perform database administration or otherwise manipulate customer data. FSAs contact the help desk as necessary if they cannot resolve a problem.

Internet—An informal collection of government, military, commercial and educational computer networks using the transmission control protocol/internet protocol (TCP/IP) to transfer information. The global collection of interconnected local, mid-level and wide-area networks that use the internet protocol as the network layer protocol.

News group—Internet resources by which individuals interested in a particular topic may read and post messages that are accessed, read and responded to by other internet users. News groups are moderated (where messages are screened for appropriateness before posting by individuals in charge of the news group) or unmoderated (where all messages are posted, regardless of content).

Page Master—The creator and, or focal point for specific material posted on the organization’s home page.

SATE —A single, integrated communications awareness, training and education effort covering communications security (COMSEC), computer security (COMPUSEC) and emission security (EMSEC) disciplines. The program emphasizes information protection precepts and promotes consistent application of security principles in the use of Air Force information systems.

Server—Software residing on an appropriate hardware platform (computer) that provides a service to other computers or programs, by satisfying client requests.

Transmission Control Protocol/Internet Protocol (TCP/IP)—The most accurate name for the set of protocols known as the "Internet Protocol Suite." TCP and IP are two of the protocols in this suite. Because TCP and IP are the best known of the protocols, it has become common to use the term TCP/IP or IP/TCP to refer to the whole family. TCP (the "transmission control protocol") is responsible for breaking up the message into datagrams, reassembling them at the other end, resending anything that gets lost and putting things back in the right order. IP (the "Internet Protocol") is responsible for routing individual datagrams.

Vulnerability—Weakness in an information system, or cryptographic system or components (e.g. system security procedures, hardware design, internal controls) that could be exploited.

Web Page—A single document that includes the text of the document, its structure, any links to other documents, images and other media.

Web Server—A software/hardware combination that provides information resources to the WWW.

Workgroup Administrator (WGA)—The WGA is normally a duty supporting a functional community (e.g., work centers, flights, squadrons or organizations) and is the first line of help customers contact to resolve problems. The WGA should be a 3A0X1 (Information Manager). Information managers receive 3/7 level training on workgroup administration, a significant part of WGA duties. When a 3A0X1 is not assigned, any AFSC or occupational series can perform WGA duties once trained and certified. WGAs are usually not assigned to the NCC, though are logically an extension of the NCC customer service team. WGAs take direction from the FSA and NCC. NCC direction takes precedence over FSA direction. WGAs possess developed knowledge of hardware, software and communications principles and install, configure and operate client/server devices. They resolve day-to-day administrative and technical system problems users experience, and should contact their FSA or NCC customer service if they cannot resolve their problem.

Attachment 2

COMPLIANCE STATUS DATA COLLECTION

Compliance Status Data Collection.

Computer	**Advisory**	**Configuration Log**

Advisory number	Computer identifier	Action taken	Date action completed

Attachment 3

CENTRALLY MANAGED SYSTEM ANTI-VIRUS STATUS LOG

Table A3.1. Centrally Managed System Anti-Virus Status Log.

Centrally	**Managed**	**System Anti-Virus**	**Status Log**
System Name	**OPR/POC**	**Action taken**	**Date action completed**

Attachment 4

FUNCTION SYSTEM ADMINISTRATOR (FSA) APPOINTMENT LETTER

MEMORANDUM FOR 436 CS/CCS

FROM: <ORGANIZATION>/CC

SUBJECT: Functional System Administrator (FSA)

1. The following individuals have been appointed to serve as FSAs for <SYSTEM NAME> in the <ORGANIZATION>

RANK/NAME	***OFF SYM***	***DUTY PHONE***	***HOME PHONE***
Primary:			
Alternate:			

2. FSAs are my primary POCs for functional computer systems in my organization. Our FSAs are familiar with our functional mission and requirements. They have also been trained on operation and administration of specific functional systems in our organization. Although not formally assigned, they take direction from the Network Control Center (NCC) on computer systems issues. Their specific areas of responsibility are outlined in AFI 33-115v1, para 6.4.5. My FSAs have read and will enforce all pertinent AFIs and NCC guidelines.

3. My FSAs, either the primary or alternate(s) will be present for duty and will make themselves available to assist NCC personnel on any computer systems issues. I will also inform my FSAs and other members of my organization that the FSAs along with WGAs are primarily the unit focal point to Communications Customer Service for computer systems or network assistance.

4. I will appoint a new FSA in writing 60 days prior to the incumbent FSA's separation/retirement, PCS or reassignment to other duties.

5. This letter supersedes all previous letters, same subject.

Signature
Commander

cc: each individual

Attachment 5

WORKGROUP GROUP ADMINISTRATOR (WGA) APPOINTMENT LETTER

MEMORANDUM FOR 436 CS/CCS

FROM: <ORGANIZATION>/CC

SUBJECT: Workgroup Group Administrator (WGA)

1. The following individuals have been appointed to serve as WGAs in the <ORGANIZATION>

RANK/NAME	***OFF SYM***	***DUTY PHONE***	***HOME PHONE***
Primary:			
Alternate:			

2. WGAs are my primary POCs for computers and limited network issues in my organization. Although not formally assigned, they take direction from the Network Control Center (NCC) on computer and network issues. Their specific areas of responsibility are outlined in AFI 33-115v1, para 6.4.6. My WGAs have read and will enforce all pertinent AFIs and NCC guidelines.

3. My FSAs, either the primary or alternate(s) will be present for duty and will make themselves available to assist NCC personnel on any computer systems issues. I will also inform my WGAs and other members of my organization that the WGAs along with FSAs are primarily the unit focal point to Communications Customer Service for computer systems or network assistance.

4. I will appoint a new FSA in writing 60 days prior to the incumbent FSA's separation/retirement, PCS or reassignment to other duties.

5. This letter supersedes all previous letters, same subject.

Signature
Commander

cc: each individual

Attachment 6

USER AGREEMENT

«Date»

INTERNET RULES:

1. I, (*Rank) (FName) (LName)*, have attended the SATE Training Course on this date, (*Date)*.

a. I understand that Department of Defense computer systems are for authorized use only and may be monitored to ensure that their use is authorized, to manage the system, to facilitate against unauthorized access and to verify security procedures, survivability and operational security.

b..I understand that using Department of Defense computer systems constitutes consent to monitoring and that all information, including personal information, may be obtained during monitoring.

c. I understand that misuse of government equipment could result in disciplinary action and/or criminal prosecution against me, which may undermine my position here at Dover Air Force Base and my military or civilian career with the government.

d. I understand that I am not to install any programs on the computer(s) assigned to me unless they are job-related and I am required by my job position and told to do so by my squadron's Workgroup Manager/Network Administrator.

E-MAIL PROTOCOLS:

1. I hereby certify that I will

a. Not send "chain letters" through the e-mail system on base.

b. Not send mass e-mail messages (messages to entire groups on base or the entire base).

c. Not use the government e-mail system to distribute offensive or disparaging material.

d. Not use the government e-mail system for unauthorized or unofficial correspondence.

BY SIGNING THIS DOCUMENT

1. I certify that I fully understand my responsibilities when using the personal computer(s) assigned to me on Dover Air Force Base.

2. I also certify that I will adhere to the "E-mail Protocols" and "Rules of the Internet" that were explained to me in this class.

_____

(FName) (LName), (Rank)